REMARKS

Claims 1-5 are pending. The Office Action dated July 18, 2008 in this Application has been carefully considered. The following remarks are presented in a sincere attempt to place this Application in condition for allowance. Reconsideration and allowance are respectfully requested in light of the above amendments and following remarks.

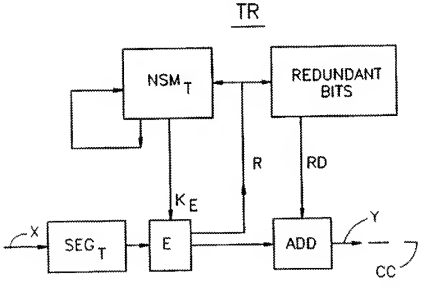
Claims 1 - 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yanovsky (U.S. Patent 5,703,948) in view of Rodriguez *et al.* (U.S. Patent 7,209,559). Claim 1, however, recites at least one of the distinguishing characteristics of the Claims, namely "generating a second key by executing a function that ***uses the first key***." (Emphasis Added).

Yanovsky does not teach that a second key is generated using the first key. Instead, Yanovsky teaches generating a new key based on random characteristics, such that each new key is not based on a prior key. In Yanovsky, segments of a plaintext message are encrypted segment by segment using a different encryption key K_E for each segment. Yanovsky, col. 4, lines 21 – 23. The encryption key K_E changes randomly segment by segment, and subsequent versions of the encryption key K_E do not depend on and are not a function of the prior versions. See Yanovsky, col. 4, lines 23 – 26. Therefore, the cited reference Yanovsky does not teach every element of Claim 1.

The portions of Yanovsky cited by the Examiner further support the position of the Applicant that Yanovksy teaches generating new keys based on random characteristics, not based on a prior encryption key K_E. First, the Examiner cites Column 4, lines 45-49 and Column 7, lines 61 – 65 as teaching the generation of a second key by executing a function that uses the first key. The cited portions, however, indicate that the normal state machine, which outputs the encryption

key K_E, changes its state ***according to a function of random bits***, not a prior version of the encryption key K_E.

The Examiner also submits that Figure 1 shows that the current encryption key K_E is fed back to the normal state machine to generate the next key. A review of Figure 1 reveals that encryption key K_E is fed as an input to encryption algorithm E, but does not show K_E fed back to the normal state machine NSM_T. See Figure 1 reproduced below. Instead, the output, random characteristic R is output and fed into new state function f_{NS} (shown in Figure 2) to produce new encrypting key K_{E+1}. See Yanovsky, col. 6, lines 62 – 67 and col., 7, lines1 – 21. Thus, Figure 1 does not show that a new encrypting key KE_{+1} is generated based on a prior key.



Yanovsky, instead, teaches that a new encrypting key K_{E+1} is produced by two inputs; neither of these two inputs is the prior encryption key K_E. See Yanovsky, col. 6, lines 62 – 67 and col., 7, lines1 – 21. The first input is the random characteristic R composed of two random bits Ri (T), which are two random bits of ciphertext Y. This ciphertext Y is an encrypted segment of a plain text message encrypted by the prior encryption key K_E. The second input is the output NORSTi of the normal state memory NST. The output NORSTi determines the locations of the random bits in the encrypted segment Yi. The new state NORSTi+1 is determined by a function of the old state $NORST_i$, plus the random bits Ri taken from the segment Yi. The new state $NORST_{i+1}$ is used to produce the new encrypting key K_{E+1}. Thus, the new encrypting key K_{E+1} is not a function of a prior key, such as K_E, but instead a function of random ciphertext bits.

Yanovsky, therefore, does not teach every element of Claim 1, namely generating a second key using a first key. The cited reference Rodriguez is not relied upon to teach generating a second key using a first key. Applicant respectfully submits that the rejection of Claim 1 is traversed and requests withdrawal of the rejection.

Claim 2 - 5 should also be allowable over the two references, at least by virtue of its dependency on Claim 1 which is believed allowable. Accordingly, Applicant respectfully submits that the rejections of Claim 2 - 5 are traversed and requests withdrawal of the rejections.

New Claim

New Claim 6, dependent on Claim 1, recites "exchanging only the first key between a receiver and a sender." Support is found, for example, on p. 5 L 7 of the Application. No new

matter is introduced. Claim 6 should be allowable over the cited references, at least by virtue of its dependency on Claim 1 which is believed allowable for the reasons discussed previously.

Applicant has now made an earnest attempt to place this Application in condition for allowance. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of Claims 1-6.

Applicant does not believe that any fees are due; however, in the event that any fees are due, the Director is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-0605 of CARR LLP.

Should the Examiner deem that any further amendment is desirable to place this application in condition for allowance, the Examiner is invited to telephone the undersigned at the number listed below.

Respectfully submitted,

CARR LLP

Dated: October 20, 2008
CARR LLP
670 Founders Square
900 Jackson Street
Dallas, Texas 75202
Telephone: (214) 760-3030
Fax: (214) 760-3003

/Gregory W. Carr/
Gregory W. Carr
Reg. No. 31,093